

AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated hereafter (where underlining “_” denotes additions and strikethrough “-” denotes deletions).

Claims:

1 – 31. (Canceled).

32. (Previously Presented) A unit that is locked against use for communications until the unit is unlocked, comprising:

memory for storing an unlock code with the unlock code being generated from an algorithm using a secret code and an identifier of the unit;

a control for receipt of an input code; and

a processor being functionally connected to the control and to the memory to effect a comparison of the input code to the unlock code, and to effect an unlocking of the unit if the comparison results in a finding that the input code is substantially equal to the unlock code.

33. (Previously Presented) The unit of Claim 32, wherein the identifier comprises an identifier unique to the unit.

34. (Previously Presented) The unit of Claim 32, wherein the identifier comprises an electronic serial number of the unit.

35. (Previously Presented) The unit of Claim 32, wherein the control is operative to receive the input code and a system identification number from a selected network; and wherein the processor is operative, after the unlocking of the unit, to effect activation of the unit on the selected network based on the system identification number.

36. (Previously Presented) The unit of Claim 32, wherein the algorithm comprises a cryptographic algorithm; and wherein the unlock code comprises a pseudo-random output generated by the cryptographic algorithm.

37. (Previously Presented) The unit of Claim 32, wherein the algorithm comprises a cave algorithm; and wherein the unlock code comprises a subset of mixing register result generated by the cave algorithm.

38. (Previously Presented) The unit of Claim 32, wherein the algorithm comprises an MD5 algorithm; and wherein the unlock code comprises a subset of an MD5 result.

39. (Previously Presented) The unit of Claim 32, wherein the algorithm used to generate the unlock code is run by a device other than the unit; and wherein the unlock code is loaded by the device in the memory.

40. (Previously Presented) The unit of Claim 32, wherein the unit comprises a wireless unit; and wherein the identifier comprises an electronic serial number of the wireless unit.

41. (Previously Presented) The unit of Claim 32, wherein the algorithm includes division of a secret code by an identifier of the unit.

42. (Previously Presented) The unit of Claim 41, wherein the division of the secret code by the identifier of the unit results in a remainder and the remainder is the secret code.

43. (Previously Presented) With respect to a unit loaded with an identifier, a method to render the unit useless for communications until the unit is unlocked, the method comprising:

generating an unlock code by using an algorithm with

a secret code and the identifier;

storing the unlock code in the unit; and

configuring the unit to be unlocked through input into the unit of an input code

substantially equal to the unlock code,

whereby the unit cannot be used for communications until the unit is unlocked

with the input of the input code substantially equal to the unlock code.

44. (Previously Presented) The method of Claim 43, wherein generating the unlock code comprises causing the unit to generate the unlock code by using the algorithm to divide the secret code by the identifier.

45. (Previously Presented) The method of Claim 44, wherein dividing the secret code by the identifier produces a remainder, and further including selecting the remainder as the unlock code.

46. (Previously Presented) The method of Claim 43, wherein the algorithm comprises a cave algorithm; and wherein generating the unlock code comprises using the cave algorithm.

47. (Previously Presented) The method of Claim 43, wherein the algorithm comprises an MD5 algorithm; and wherein generating the unlock code comprises using the MD5 algorithm.

48. (Previously Presented) The method of Claim 43, further comprising:
receiving a system identification number from a selected network; and
based on unlocking of the unit, activating the unit on the selected network.

49. (Previously Presented) With respect to a unit that has been loaded with an identifier and that has been locked, a method to unlock the unit for communications, comprising:

generating an unlock code using an algorithm with a secret code and an identifier;

receiving an input code;

comparing the input code to the unlock code; and

unlocking the unit if the input code is substantially equal to the unlock code.

50. (Previously Presented) The method of Claim 49, wherein generating the unlock code comprises causing the unit to generate the unlock code by using the algorithm to divide the secret code by the identifier. to obtain a remainder, and to select the remainder as the unlock code.

51. (Previously Presented) The method of Claim 49, wherein dividing the secret code by the identifier produces a remainder, and further including selecting the remainder as the unlock code.

52. (Previously Presented) The method of Claim 49, further including:
receiving a system identification number from a selected network; and
based on the unlocking of the unit, activating the unit on the selected network.

53. (Previously Presented) The method of Claim 49, wherein receiving the input code comprises receiving the input code from a selected network; and further including:

receiving a system identification number from the selected network; and
based on the unlocking of the unit, activating the unit on the selected network.

54. (Previously Presented) The method of Claim 49, wherein generating the unlock code comprises causing the unlock code to be generated by a device other than the unit.

55. (Previously Presented) A computer-readable medium on which is stored a computer program for rendering a unit useless for operation until the unit is unlocked, the unit having an identifier unique to the unit, the computer program comprising instructions, which when executed by a computer perform:

obtaining a secret code;
using the secret code with the identifier in an algorithm to generate an unlock
code;
loading the unit with the unlock code; and
configuring the unit so that the unit can only be unlocked through input into the
unit of an input code substantially equal to the unlock code.

56. (Previously Presented) The computer-readable medium of Claim 55, wherein the algorithm comprises a cave algorithm; and wherein using the secret code with the identifier in the algorithm to generate the unlock code comprises using the secret code with the identifier in the cave algorithm to generate the unlock code.

57. (Previously Presented) The computer-readable medium of Claim 55, wherein the algorithm comprises an MD5 algorithm; and wherein using the secret code with the identifier in the algorithm to generate the unlock code comprises using the secret code with the identifier in the MD5 algorithm to generate the unlock code.

58. (Previously Presented) The computer-readable medium of Claim 55, wherein the algorithm comprises division of the secret code by the identifier of the unit.

59. (Previously Presented) The computer-readable medium of Claim 58, wherein the division of the secret code by the identifier of the unit results in a remainder and the remainder is the secret code.

60. (Previously Presented) A method of controlling use of a communications unit having an identifier, the method comprising:

- configuring the communication unit to be lockable;
- configuring the communication unit to be unlockable; and
- generating an unlock code for the communication unit using at least the identifier, wherein the unlock code is used to change the state of the communication unit from locked to unlocked.

61. (Previously Presented) The method of claim 60, wherein generating an unlock code for the communication unit further includes:

- using an algorithm and a secret code in conjunction with the identifier.

62. (Previously Presented) The method of claim 61, wherein the algorithm is a cryptographic function.

63. (Previously Presented) The method of claim 62, wherein the cryptographic function is a hash function.

64. (Previously Presented) The method of claim 62, wherein the cryptographic function is a checksum function.

65. (Previously Presented) The method of claim 60, wherein the step of generating further includes the step of:

using a secret code and at least the identifier in a mathematical operation to generate the unlock code.

66. (Previously Presented) The method of claim 65, wherein the mathematical operation is division, and the secret code is divided by the identifier.

67. (Previously Presented) The method of claim 66, wherein the secret code is related to the remainder.

68. (Previously Presented) The method of claim 67, wherein the remainder is padded, and the padded remainder is the secret code.

69. (Previously Presented) The method of claim 67, wherein the remainder is the secret code.

70. (Previously Presented) The method of claim 67, wherein the communication unit cannot be used for communications responsive to the communication unit being in a locked state.

71. (Previously Presented) The method of claim 67, wherein the communication unit can be used for communications responsive to the communication unit being in an unlocked state.

72. (Previously Presented) A lockable/unlockable communication unit, the communication unit comprising:

a memory having unlock code stored therein, the unlock code generated using at least the identifier;

a control adapted to receive a input code; and

a processor in communication with the control and the memory, the processor adapted to compare the unlock code with the input, and responsive to the input being substantially equal to the unlock code, the processor effects a change of state from locked to unlocked.

73. (Previously Presented) The unit of claim 72, wherein the identifier comprises an identifier unique to the unit.

74. (Previously Presented) The unit of claim 72, wherein the identifier comprises an electronic serial number of the unit.

75. (Previously Presented) The unit of claim 72, wherein the communication unit is unable to communicate when the communication unit is in a locked state.

76. (Previously Presented) A system for controlling use of a communication unit, the system comprising:

means for configuring the communication unit to be lockable;

means for configuring the communication unit to be unlockable; and

means for generating an unlock code for the communication unit using at least the identifier, wherein the unlock code is used to change the state of the communication unit from locked to unlocked.

77. (Previously Presented) The system of claim 76, wherein the means for generating the unlock code uses an algorithm and a secret code in conjunction with the identifier.

78. (Previously Presented) The system of claim 77, wherein the algorithm is a cryptographic function.

79. (Previously Presented) The system of claim 78, wherein the cryptographic function is a hash function.

80. (Previously Presented) The system of claim 78, wherein the cryptographic function is a checksum function.

81. (Previously Presented) The system of claim 76, wherein the means for generating the unlock code uses a secret code and at least the identifier in a mathematical operation to generate the unlock code.

82. (Previously Presented) The system of claim 81, wherein the mathematical operation is division, and the secret code is divided by the identifier.

83. (Previously Presented) The system of claim 82, wherein the secret code is related to the remainder.

84. (Previously Presented) The system of claim 83, wherein the remainder is padded, and the padded remainder is the secret code.

85. (Previously Presented) The system of claim 83, wherein the remainder is the secret code.

86. (Previously Presented) The system of claim 76, wherein the communication unit cannot be used for communications responsive to the communication unit being in a locked state.

87. (Previously Presented) The system of claim 76, wherein the communication unit can be used for communications responsive to the communication unit being in an unlocked state.

88. (Previously Presented) A computer-readable medium on which is stored a computer program for controlling use of a communication unit having an identifier, the computer program comprising instructions, which when executed by a computer perform:

configuring the communication unit to be lockable;

configuring the communication unit to be unlockable; and

generating an unlock code for the communication unit using at least the identifier, wherein the unlock code is used to change the state of the communication unit from locked to unlocked.

89. (Previously Presented) The computer-readable medium of Claim 88, wherein generating an unlock code for the communication unit further includes:

using an algorithm and a secret code in conjunction with the identifier.

90. (Previously Presented) The computer-readable medium of claim 89, wherein the algorithm is a cryptographic function.

91. (Previously Presented) The computer-readable medium of claim 90, wherein the cryptographic function is a hash function.

92. (Previously Presented) The computer-readable medium of claim 90, wherein the cryptographic function is a checksum function.

93. (Previously Presented) The computer-readable medium of claim 88, wherein generating an unlock code for the communication unit further includes:

using a secret code and at least the identifier in a mathematical operation to generate the unlock code.

94. (Previously Presented) The computer-readable medium of claim 93, wherein the mathematical operation is division, and the secret code is divided by the identifier.

95. (Previously Presented) The computer-readable medium of claim 94, wherein the secret code is related to the remainder.

96. (Previously Presented) The computer-readable medium of claim 95, wherein the remainder is padded, and the padded remainder is the secret code.

97. (Previously Presented) The computer-readable medium of claim 95, wherein the remainder is the secret code.